

# Chapter 14

## Configure Encryption Interfaces

The Internet Protocol security architecture (IPSec) provides a security suite for the IPv4 and IPv6 network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and non-repudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates.

IPSec defines a security association (SA) and key management framework that can be used with any network layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. For more information, see the *JUNOS Internet Software Configuration Guide: Getting Started*. The standards are defined in the following RFCs:

RFC 2401, *Security Architecture for the Internet Protocol*

RFC 2406, *IP Encapsulating Security Payload (ESP)*

To enable encryption interfaces, you can configure the following properties:

Configure the Tunnel Address on page 223

Specify the Security Association Name on page 224

Configure Traffic on page 224

Configure MTU for Encryption Interfaces on page 225

### Configure the Tunnel Address

Secure traffic travels through tunnel interfaces between remote hosts. You configure each IPSec tunnel as a logical interface on the ES PIC. As you do with other tunnel interfaces, include the tunnel statement at the [edit interfaces es-fpc/pic/port unit *logical-unit-number*] hierarchy level to specify the source and destination addresses:

```
[edit interfaces]
es-fpc/pic/port {
    unit logical-unit-number {
        tunnel {
            source address;
            destination address;
        }
    }
}
```



IPSec runs in two modes: transport and tunnel. The ES PIC supports the tunnel mode only. For information about IPSec modes, see the *JUNOS Internet Software Configuration Guide: Getting Started*.

The ES PIC does not automatically reassemble if the tunnel breaks.

## Specify the Security Association Name

The security association is the set of properties that defines the protocols for encrypting internet traffic. To configure encryption interfaces, you specify the security association (SA) name associated with the interface by including the `ipsec-sa sa-name` statement at the [edit interfaces *es-fpc/pic/port unit logical-unit-number family inet*] hierarchy level:

```
[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]
  ipsec-sa sa-name;
```

For information about configuring the security association, see the *JUNOS Internet Software Configuration Guide: Getting Started*.

## Configure Traffic

You use firewall filters to configure traffic to flow through an IPSec tunnel. To configure inbound and outbound traffic for an IPSec tunnel, include the filter statement at the [edit firewall] hierarchy level:

```
[edit firewall]
  filter inbound-decrypt-filter;
  filter outbound-encrypt-filter;
```

To ensure outbound traffic is transmitted on the appropriate interface, include the filter and output statements at the [edit interfaces *interface-name unit logical-unit-number family inet*] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet]
  filter {
    output outbound-encrypt-filter;
  }
```

To ensure inbound traffic is received on the appropriate interface, include the filter and input statements at the [edit interfaces *interface-name unit logical-unit-number family inet*] hierarchy level:

```
[edit interfaces]
  interfaces interface-name {
    unit logical-unit-number {
      family inet {
        filter {
          input inbound-decrypt-filter;
        }
      }
    }
  }
```

For detailed information on configuring traffic for an IPSec tunnel, see the *JUNOS Internet Software Configuration Guide: Getting Started*. For detailed information on firewalls, see the *JUNOS Internet Software Configuration Guide: Policy Framework*.

## Configure MTU for Encryption Interfaces

The protocol MTU value for encryption interfaces must always be less than the default interface MTU value of 3900 bytes; the configuration fails to commit if you select a greater value. To set the MTU value, include the `mtu bytes` statement at the [`edit interfaces interface-name unit logical-unit-number family inet`] hierarchy level:

```
[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]
  mtu bytes;
```

For more information, see “Set the Protocol MTU” on page 131.

### **Example: Configure Encryption Interfaces**

Configure two logical interfaces: unit 0 has a manual SA with static keys and algorithms, and unit 1 has a dynamically negotiated SA:

```
[edit interfaces]
es-0/0/0 {
  unit 0 {
    tunnel {
      source 10.36.17.4;
      destination 10.36.15.3;
    }
    family inet {
      ipsec-sa manual-sa1;
    }
  }
  unit 1 {
    tunnel {
      source 10.36.16.4;
      destination 10.36.12.7;
    }
    family inet {
      ipsec-sa dynamic-sa1 {
    }
  }
}
```

- Configure a manual SA with specified keys, including direction, protocol, Security Parameter Index (SPI), authentication, and encryption:

```
[edit security ipsec]
security-association manual-sa1 {
    manual {
        direction bidirectional {
            protocol esp;
            spi 2312;
            authentication {
                algorithm hmac-md5-96;
                key ascii-text 1234123412341234;
            }
            encryption {
                algorithm 3des-cbc;
                key ascii-text 123456789009876543211234;
            }
        }
    }
}
```

- Configure a dynamic SA with an IKE proposal, IKE policy, IPSec proposal, IPSec policy, and an SA associated with an IPSec policy:

```
[edit security]
ike {
    proposal ike-proposal {
        authentication-method pre-shared-keys;
        dh-group group1;
        authentication-algorithm sha1;
        encryption-algorithm 3des-cbc;
    }
    policy 10.1.1.2 {
        mode main;
        proposal ike-proposal;
        pre-shared-key ascii-text example-pre-shared-key;
    }
}
ipsec {
    policy dynamic-policy-1 {
        proposal [dynamic-1];
    }
    proposal dynamic-1 {
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
        protocol esp;
    }
    security-association dynamic-sa1 {
        dynamic ipsec-policy dynamic-policy-1;
    }
}
```

Configure firewall filters that define outbound traffic for the IPSec tunnel and ensure that the tunneled traffic goes out the appropriate interface.

```
[edit firewall]
filter ipsec-encrypt-policy-filter {
    term term1 {
        from {
            source-address { 10.1.1.0/24; } // local network
            destination-address { 10.2.2.0/24; } // remote network
        }
        then ipsec-sa manual-sa1; // apply SA name to packet
    }
    term term2 {
        then accept;
    }
}

[edit interfaces]
fe-0/0/1 {
    unit 0 {
        family inet {
            filter {
                input ipsec-encrypt-policy-filter;
            }
            address 10.1.1.254/24;
        }
    }
}
```

Configure firewall filters that define inbound traffic for the IPSec tunnel and ensure that the appropriate interface receives the tunneled traffic:

```
filter ipsec-decrypt-policy-filter {
    term term1 {
        from {
            source-address { 10.2.2.0/24; } // remote network
            destination-address { 10.1.1.0/24; } // local network
        }
        then accept;
    }
    term term2 {
        from {
            source-address { 10.5.5.5; } // tunnel source address
            destination-address { 10.6.6.6; } // tunnel destination address
            protocol esp;
        }
        then accept;
    }
}
```

```
• [edit interfaces]
• es-1/2/0 {
•   unit 0 {
•     tunnel {
•       source 10.5.5.5;           // tunnel source address
•       destination 10.6.6.6;      // tunnel destination address
•     }
•     family inet {
•       filter {
•         input ipsec-decrypt-policy-filter;
•       }
•       ipsec-sa manual-sa1;
•       address 10.1.1.8/32 {
•         destination 10.2.2.254; // SA name applied to packet
•         // local interface address inside local VPN
•         // destination address inside remote VPN
•       }
•     }
•   }
• }
```